

SANDY CITY
APPROVED CLASS SPECIFICATIONS

I. <u>Position Title:</u> IT Cyber Security Analyst	<u>Revision Date:</u> 07/19 <u>EEO Category:</u> Technician <u>Status:</u> Exempt (Comp) <u>Control No:</u> 30377
---	--

II. Summary Statement of Overall Purpose/Goal of Position:

Under the direction of the Information Technology Director, performs cyber security operations, planning, prevention, response and maintenance.

III. Essential Duties:

- Research, develop and implement IT security standards and best practice policies and procedures.
- Monitor computer networks for security issues.
- Configure, and maintain security monitoring software.
- Perform cybersecurity planning process and gather information to implement detailed NIST operational supporting requirements.
- Ensure compliance to security standards and policies, monitoring access privileges, conducting risk assessments, investigation of breaches, suspicious activities, and remediation of identified security threats or risks, and breaches.
- Provide IT security training to users.
- Be knowledgeable on cyber security trends and measures to mitigate breaches.
- Responsible for insuring City is Payment Card Industry (PCI) compliant.
- Create and update standard security documentation, system description, security plan, contingency plan, and other plans as required for federal or State security audits.

IV. Marginal Duties:

- Perform other duties as assigned.

V. Qualifications:

Education: Requires bachelor's degree in computer science, cyber security or related field.

Experience: Proven track record of supporting customers in cyber security issues. May substitute on a year for year basis any equivalent combination of education and experience. Knowledge of tools used for network security (DLP, NIPS, WAF, HIPS, AV, Firewalls, etc.)

Certifications/Licenses: Requires a valid Utah Driver's License. Must possess at least one cyber security related certification.

Probationary Period: A one-year probationary period is required for this position.

Knowledge of: LAN, WAN, wireless networking, VMware, routers, UNIX and Windows operating systems and application software including security, regulatory compliance standards, patch management and database management.

Responsibility for: Responsible to oversee security aspects of: connected mobile devices, network security monitoring software, Network Servers, Firewall and Routers; responsibility for the care, condition and use of expensive City computer equipment.

Communication Skills: Ability to clearly communicate verbally and in writing. Able to tactfully walk users through spotting red flags in cyber security attacks, recognizing bad URL's and general cyber security training.

Tool, Machine, and Equipment Operation: Requires use of Thin Clients, PCs, printers, routers, servers and telephone system.

Analytical Ability: Ability to determine underlying causes of security issues. Troubleshoot and configuring software systems over the phone. Operate a variety of computer equipment and software; understand and follow oral and written instructions.

VI. Working Conditions:

Physical Demands: While performing duties of job, employee typically handles office equipment, objects or controls; may periodically bend, stoop or crouch. Employee will sit or stand for long periods of time and move objects up to 20 pounds.

Work Environment: Employee will generally work in a comfortable office setting with occasional exposure to inclement weather conditions. The noise level in the work environment is usually minimal. Moderate mental effort is required daily; some pressure is generated by contact with other departments and exposure to deadlines.

The above statements are intended to describe the general nature and level of work being performed by the person(s) assigned to this job. They are not intended to be an exhaustive list of all duties, responsibilities and skills required of personnel so classified. The approved class specifications are not intended to and do not infer or create any employment compensation or contract rights to any person or persons. This updated job description supersedes prior descriptions for the same position. Management reserves the right to add or change duties at any time.

DEPT/DIVISION APPROVED BY: _____ DATE: _____

PERSONNEL DIV APPROVED BY: _____ DATE: _____